AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

- One (1) 64 GB Monster Digital thumb drive
- RCA tablet, model RCT6203W46, Serial Number LA161EL1B3941
- HP laptop, Serial Number 5CG3162TKQ

Case No. MJ 15-386

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

One (1) 64 GB Monster Digital thumb drive, RCA tablet, and HP laptop as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § (2252 (a)(2)	receipt and distribution of child pornography
Title 18, U.S.C. § (2252(a)(4)(B)	possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

INGRID ARBUTHNOT-STOHL, SPECIAL AGENT FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: August 21, 2015

Judge's signature

City and state: Seattle, Washington

JAMES P. DONOHUE, CHIEF U.S. MAGISTRATE JUDGE
Printed name and title

2015R00955

AFFIDAVIT

STATE OF WASHINGTON)
)
COUNTY OF KING)

I, Ingrid Arbuthnot-Stohl, being duly sworn, state:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since December 2010. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252A, 2422, and 2423. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in numerous forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. The statements contained in this affidavit are based in part on information provided by law enforcement officials and others known to me, and on my experience and background as a law enforcement officer. Since the affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I

believe are necessary to establish probable cause to believe that violations of Title 18, United States Code, §§ 2252(a)(2) and 2252 (a)(4)(B), have been committed and that the instrumentalities, fruits, and evidence of those crimes will be found in a particular place to be searched.

3. This affidavit is made in support of a search warrant for the following items, which are currently in the legal custody of FBI/Seattle:

- **One (1) 64 GB Monster Digital thumb drive**
- **RCA tablet, model RCT6203W46, Serial Number LA161EL1B3941**
- **HP laptop, Serial Number 5CG3162TKQ**

The devices listed above were voluntarily surrendered and subsequently seized from the residence of MICHAEL GREENLEAF on August 13, 2015, and are currently stored at the FBI Headquarters office, located in Seattle, Washington. The devices listed above will be referred to in this Affidavit as "SUBJECT DEVICES," (described in Attachment A, hereto).

4. I am submitting this affidavit in support of a search warrant authorizing a search of the SUBJECT DEVICES and the extraction from the SUBJECT DEVICES of electronically stored content and information described in Attachment B hereto, which content and information constitute instrumentalities, fruits, and evidence of the foregoing violations.

5. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

6. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

II. BACKGROUND TO INVESTIGATION

7. In November 2014, FBI Tampa executed a search warrant at the residence of Kevin Reynolds in Winter Springs, Florida. At the time of the search warrant, Kevin Reynolds was in the process of downloading child pornography to an encrypted external hard drive. During the investigation, it was revealed that Kevin Reynolds sent money, using Western Union, to Russia for the production of child pornography that included identifiers to ensure the child pornography was produced specifically for him. As a result of this investigation, in December 2014, FBI Tampa sent a subpoena to Western Union requesting transaction records for identified subjects in Russia and the Ukraine.

8. In December 2014, FBI Tampa received confirmation that MICHAEL GREENLEAF sent money via Western Union on or about July 24, 2013, to one of the identified subjects. MICHAEL GREENLEAF supplied Western Union with a contact address of 214 Summit Ave E. #406, Seattle, WA 98102. Open source checks revealed that the above address is a previous address for MICHAEL GREENLEAF.

III. PROBABLE CAUSE

9. On August 13, 2015, SA Ingrid Arbuthnot-Stohl and SA Steven Vienneau contacted MICHAEL GREENLEAF at his current address of 7 Harrison St., Apt. 25, Seattle, WA 98109 to ask him about the Western Union transaction. During the interview, MICHAEL GREENLEAF stated that he used a tablet that belonged to his mother, M.G. SA Arbuthnot-Stohl and SA Vienneau requested permission from M.G. to conduct a preliminary forensic examination on the tablet to confirm there was no child pornography stored on the device. M.G. signed a consent to search computer form, and allowed MICHAEL GREENLEAF to supervise the examination of the tablet.

10. During the examination of the tablet, Agents discovered three website addresses, two of which included the word "ped". Based upon my knowledge and experience, I know that "ped" is a common term used by those who engage in child pornography to refer to "pedophile", "pedophilia", or other similar word. When asked about the websites, MICHAEL GREENLEAF admitted that he viewed child pornography using the tablet, as well as a laptop computer, and thumb drive (the SUBJECT DIGITAL DEVICES) that were located in the residence, 7 Harrison St., Apt. 25, Seattle, WA 98109. MICHAEL GREENLEAF stated that he understood child pornography to be images and videos of males and females under the age of 18 who are engaged in sexual activities. MICHAEL GREENLEAF stated that he received sexual gratification from viewing child pornography. MICHAEL GREENLEAF stated that he has downloaded thousands of images and videos of child pornography to the laptop and thumb drive, and has viewed child pornography on the tablet.

11. Based upon the above statement by MICHAEL GREENLEAF, Agents seized the SUBJECT DEVICES. MICHAEL GREENLEAF retrieved the items from his own residence and surrendered them to Agents. The SUBJECT DEVICES are currently stored in the FBI Headquarters Office in Seattle, WA.

12. On August 14, 2015, I learned from M.G. that both the laptop and tablet belong to her, and she revoked her consent for a law enforcement search of the tablet.

IV. TECHNICAL BACKGROUND

13. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain

access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

14. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is collected, distributed, and produced. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these images was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership based/subscription based websites to conduct business, allowing them to remain relatively anonymous.

15. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography as described below.

16. Producers of child pornography can now produce both still and moving images directly from the average video or digital camera. These still and/or moving images are then uploaded from the camera to the computer, either by attaching the camera to the computer through a USB cable or similar device, or by ejecting the camera memory card from the camera and inserting it into a card reader. Once uploaded to the computer, the images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to those by which a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Producers of child pornography can also use a scanner to transfer printed photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

17. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers, including ISPs, allow email service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet. Having said that, however, this application does not seek to reach any host computers. This application seeks permission only to search the SUBJECT DEVICES.

18. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography, and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the

world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the distributor's/recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the distributor/recipient.

19. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage elsewhere. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

20. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years.

d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

21. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another.

22. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

23. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that for the SUBJECT DEVICES, there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to

these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. FBI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

24. Because the laptop and tablet are known to be owned by M.G., there may be information on the devices belonging to an individual not suspected of a crime. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

V. CONCLUSION

25. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (Production of Child Pornography), § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are stored on the SUBJECT DEVICES. I therefore request that the court issue a warrant authorizing a search of the listed SUBJECT DEVICES for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

Dated this 21st day of August, 2015.

Ingrid Arbuthnot-Stohl, Affiant
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 21st day of August, 2015.

JAMES P. DONOHUE
Chief United States Magistrate Judge

ATTACHMENT A

The following SUBJECT DEVICES:

- **One (1) 64 GB Monster Digital thumb drive**
- **RCA tablet, model RCT6203W46, Serial Number LA161EL1B3941**
- **HP laptop, Serial Number 5CG3162TKQ**

which are currently stored in the FBI Headquarters Office, located in Seattle, Washington.

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents. files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251 (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT DEVICES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

3. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

7. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

8. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

9. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

10. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

12. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

12. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

13. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

14. Evidence of times the digital device(s) was used;

15. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

16. Evidence of Western Union transfers or other money transfers or other form of payment for child sexual exploitation materials.